Commonwealth Information Security Council
Identity and Access & Account Management Meeting
July 21, 2008
2:00-3:30pm
Washington Conference Room CESC

IAM Committee members attending:
Maria Batista, DMV
John Willinger, DMHMRSAS
Marie Greenberg, SCC
Jon Smith, VITA
Jim Lewis, ABC

IAM Committee members absent:
Mike Garner, TAX
James Austin, VDOT
Daniel Boersma, VEAP
Joel McPherson, DSS
Christopher Nicholl, DMV
Easton Rhodd, VITA
Todd Richardson, DMME
Ajay Rohatgi, VEAP

Also attending:
Peggy Ward, VITA

Introduction of new members:

- Jon Smith (VITA) and Jim Lewis (ABC) were introduced to the committee.
- Background information on the on the IAM Trust Model and IAM Committee was discussed for the new members.

IAM Part II Proposal Review:

- Background information on the original and revised proposal from Chris Nicholl was discussed.
- IAM Committee went through the revised proposal line for line. Chris Nicholl could not attend this month so we will discuss further next month when he is in attendance. Below is the original proposal with our review comments and markups in red.

1. Identify the different types of Systems that Identity Federation and Identity Synchronization can occur in. There should be at least two types of IAM systems, those with sophisticated schema capabilities and/or tracking attributes, and those that do not support identifiable attributes. Focused too much on IT

2. What items need to be defined to perform Federation or Synchronization. Focused too much on IT

3. When Federation or Synchronization [between systems] is implemented between two independent systems-

    a) Identification of, documentation, and agreement of roles should be in place between ITRM Roles and any specific Agency roles.

b) The System Owners of each system will agree on what links are acceptable between the systems.

c) Identified IT Auditors will define what auditing requirements should be implemented

d) The System Owners will define and provide to the other System Owner who are the authorized individuals that can approve changes within the systems themselves and to the synchronization configuration.

e) A documented change control process will be defined and available to appropriate individuals to both systems so that there is full understanding of what changes are proposed to each system. Only changes that effect the Identity Access Management

~~f) The System Owners will provide to each other, the documentation of how Disaster Recovery is handled within their system and how to react to Synchronization or Federation failures.~~

~~g) The System Owners will collectively decide where Documentation of System configuration artifacts will be stored and communicate this information to each other.~~

h) Documentation will be maintained collectively to define
- How are the IAM Trust Model levels mapped to accounts within the systems
- How entities identified between systems
- How roles within the systems are identified
- What are the acceptable credentials within the systems
- How are Service levels of systems tracked/enforced [what are service levels? Service accounts?]
- How are Identities tracked to the Person they are assigned to
- How are Service Accounts utilized and configured
- How rights to data are managed within the systems
- ~~How are data breach notifications are handled~~
- How the provisioning/deprovisioning of user accounts are managed within the systems

- Discussion about Memorandum of Understanding (MOU) between entities that are sharing data. Many of the point above should be place in a document that the parties agree upon to ensure understanding of the roles and requirements of the parties involved.